EnforcIT

Defense-in-Depth Solutions for Protecting Critical Information

FPGA Based Anti-Tamper

To reach the highest levels of security, using a single type of protection mechanism is inadequate. Layers of security must be employed, and higher levels of security can be achieved by moving those layers into hardware. EnforcIT® raises the achievable level of protection with technology rooted in firmware. This technology is provided in the following EnforcIT security suites:

Cryptography Suite

Customizable, FIPS-certified cryptographic cores enabling encryption, decryption, signing, and verifying of sensitive data and code.

Firmware Protection Suite

Independently configurable firmware protection mechanisms that protect critical technologies and intellectual property in your field programmable gate array (FPGA) against reverse engineering and tampering.

System-Level Security

The Cryptography Suite is a selection of NSA Suite B, FIPS-certified IP cores used to implement cryptographic operations in firmware and offload cryptographic operations from software. Users have access to AES, public key algorithms including ECC and RSA, and secure hashing including SHA-1 and SHA-2. Additionally, a random number generator is included to seed cryptography cores or to supply your own design with random data.

The Firmware Protection Suite is a selection of IP cores that implement protection mechanisms in FPGAs. With these cores, users can protect their critical technology and intellectual property against unauthorized debugging, ensure clock integrity, authenticate end-point nodes, boot devices securely, provide FPGA tamper responses, and utilize numerous other standalone FPGA security features to prevent both static and dynamic reverse engineering, tampering, and counterfeiting attacks.

EnforcIT Add-ons are additional protection technologies that interact with other EnforcIT security mechanisms to further increase the level of defense. Available enhancements include software protection integration with Microsemi's CodeSEAL™ product and the ability to create device-specific encryption keys and prevent cloning of FPGA devices using a mature, robust, and reliable physically unclonable function (PUF).

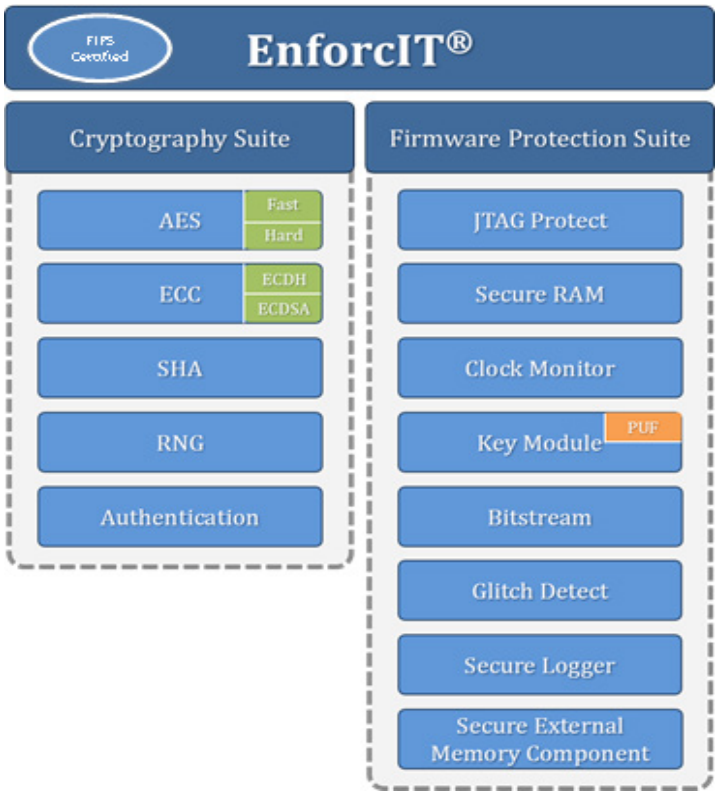

Figure 1: EnforcIT IP Suites

EnforcIT IP cores can be used in stand-alone format or combined with other cores and suites to provide additional firmware protection capabilities.

EnforcIT secures FPGA-based devices using standalone protection mechanisms and Suite B, FIPS-certified crypto cores.

NIST Certifications

Advanced Encryption Standard (AES)	Validation # 2390, 2389
Elliptic Curve Digital Signature Algorithm (ECDSA)	Validation # 393
Keyed-Hash Message Authentication Code (HMAC)	Validation # 1466
Secure Hash Standard (SHS)	Validation # 2035

EnforcIT

Defense-in-Depth Solutions for Protecting Critical Information

How EnforcIT Works

EnforcIT is distributed as a customizable set of one or more netlists (VHDL can be provided in certain situations). The anti-tamper mechanisms are inserted into your firmware bitstream to provide protection customized specifically to your systems' security and performance requirements.

Table 1: The EnforcIT Advantage

EnforcIT Features	EnforcIT Benefits
FIPS-Certified Crypto	Cryptographic IP cores are FIPS-certified, allowing you to build Suite B cryptography into your system without going through a costly, lengthy certification process.
Prevents Counterfeiting	Using unique functions intrinsic to individual manufactured hardware devices, users can generate an encryption key that only works with a single FPGA.
Multi-Layered Protection	The combination of software and hardware communicating with each other to secure your system raises the level of sophistication and cost of tools required for an adversary to attack.
Software Anti-Tamper Acceleration	EnforcIT minimizes the performance impact on software by offloading cryptographic and anti-tamper protection mechanisms into the FPGA.
Broad FPGA Device Family Support	EnforcIT provides straightforward integration into existing systems with support for Microsemi SmartFusion® and IGLOO®, Xilinx Virtex and Spartan, and Altera Cyclone and Stratix device families.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com